The CMMC Niche for a Managed Service Provider

A whitepaper by Janet Himmelreich, CMMC/RP, RPA Managing Director, 3Comply.
Janet.himmelreich@3Comply.com
www.3Comply.com or cmmc_help@3comply.com.

Synopsis

This whitepaper discusses a major business opportunity for Managed Services Providers (MSPs) in light of the CMMC 2.0 requirements. It covers what you need to know, how to identify the opportunities, and most importantly, some of the techniques we have discovered that could work for an MSP with multiple types of clients.

It is 3Comply's belief that CMMC Level 1 (Basic) will become the easy to identify minimum requirement for cyber-hygiene that every MSP must be able to demonstrate to any client – private or public. Early adopters of Level 2 (Advanced) in the CMMC hierarchy will have the advantage and the "stickiness" of having put the advanced environment in place. Combining this with knowing what needs to be done for a client to help them "inherit controls" will go a long way toward retaining a current one or gaining new ones in the public sector. Although the DoD has taken the lead in determining how it will protect its specific information, all agencies in the US Federal government Executive Branch are required to securely protect Controlled Unclassified Information (CUI). Many agencies are expected to adopt CMMC. Keep in mind in the DIB alone there are 220,000 - 300,000 DoD contractors. To start, all you need is one request to provide a CMMC compliant operation (or the desire to do so) and you can begin to carve out a niche for your MSP to be very successful in this market.

Read on for some key information to make the business case for your MSP to be an early adopter of the CMMC Level 2 cybersecurity environment.

3 things to know about 3Comply:

3Comply's philosophy and method emphasizes how to Comply Simply

The approach taken is designed so that MSP personnel remain focused on their "day job;" this way, their time is used for approval and decision making rather than writing and researching.

3Comply is an advisor and partner where work is performed by the principals directly who want to develop and maintain a long-term relationship, not a one and done consulting job.

Overview

The opportunities for Managed Service Providers (MSPs)to create a niche in the world of Cybersecurity Maturity Model Certification 2.0 (CMMC) are phenomenal, in our view. MSPs are an essential part of today's IT enterprise environments. Many companies within the Defense Industrial Base (DIB) utilize Software as a Service (SaaS) providers or IT Managed Service Providers (MSPs) that provide everything from help desk to full provision of all IT services including cybersecurity. These providers should be expected to provide at least the same level of security controls internally as is required of their customer. SaaS providers are categorized as Cloud Service Providers (CSPs), a subcategory of MSPs. Thus, any organization using SaaS services, or any other type of MSP is dependent on that provider to meet many of the practices or controls required to become CMMC compliant. The Department of Defense has identified MSPs as integral to IT environments and is planning to introduce specific rules for MSP's. In fact, it has been reported that the DoD would like to identify MSPs willing to meet the MSP rules – reported to be a cross between FedRAMP and CMMC to be able to point members of the DIB to MSPs that clearly already meet the requirements. This is a huge opportunity in our view!

In our experience, there are few MSPs that have taken the time to look at the requirements and understand their responsibilities in this supply chain. Like many companies, MSPs are waiting for the rules to be formalized before making a move. However, there are some that have clients operating in the DIB that have already stated that the MSP needs to meet the same CMMC requirements, at the same Level, for them to remain a client of that MSP. Many more have yet to discover just how they are reliant upon the MSP(s) in their environment to meet these requirements and will need a CMMC Level 2 certified MSP.

6 Things an MSP leader should know about CMMC

1. Training appropriate staff while implementing requirements, produces evidence of a program underway; by showing training records (and artifacts being created) it will help retain current clients and assist to satisfy future clients
2. Managed Service Providers (MSP) are attracting special attention in the world of CMMC – specific rules are expected in the rulemaking when it is submitted to Office of Management and Budget (OMB); these are expected to be a combination of FedRAMP and CMMC and will enable the DOD to identify MSPs that already meet requirements – a HUGE advantage
3. CMMC, based on NIST 800-171, is for Department of Defense contracts; similar cybersecurity requirements flow through the entire Executive Branch. Many state and local governments use the same or similar standards.
4. While rule making is significantly held up, our experience is that there is much more attention to the DFARS 7012 procurement clause that is required in most DOD solicitations and have been since 2017; requiring protection of CUI
5. MSPs that are ready will have a big lead in being able to offer services that are CMMC attested to for Level 1 and ready for certification at Level 2 - a big market upside
6. Level 1 maturity is appealing to protect private company information AND intellectual property

MSPs are attracting special attention.

Managed Service Providers (MSPs) and particularly, Managed Security Service Providers (MSSPs) have enormous opportunities as well as responsibilities in the cyber-readiness of US industry. This may seem like an overstatement, however, almost every sized company uses some type of managed service provider – be it a Cloud Service Provider (CSP), a tool or system that is available and used as Software as a Service (SaaS) deployed in a cloud environment or using an MSP to provide IT services that are not part of a company's core vision or mission. (Within the CMMC technical jargon MSP's, MSSP's, CSPs, and SaaS providers are all considered External Service Providers (ESP))

Certainly, companies that contract with government agencies – whether federal, state, or local, and whatever size, from very small to very large, are part of this mix. As a result, ESPs are part of the life of these companies. In fact, government regulators have caught up to the realities of operations in 2023 and beyond and are looking at ways to greatly improve the cyber-readiness of ESPs including those that provide security services. This makes sense, as Organizations Seeking Certification (OSCs in CMMC parlance) need to inherit the controls from their service providers and monitor them as they do not perform that service themselves. Ultimately the protection of government information protects the warfighter, our allies, and the country.

Niche Considerations

Basics of the Opportunity for MSPs

- CMMC Level 2 certification presents an interesting, and potentially very significant, opportunity for MSPs, particularly those focused on small to medium size enterprises that make up the bulk of the DIB. Approximately 220,000 (other cites are up to 300,000) companies are members of the DIB. Of these, more than 75% are small to medium sized.
- The DoD has described the proposed rulemaking for MSPs as requiring that a combination of FedRAMP and CMMC requirements be met. Leadership hopes that having MSPs that are specifically certified as meeting the requirements will then be readily available for members of the DIB to choose to work with and know they will be compliant. Clients will be looking for MSPs and particularly MSSPs to help them meet the requirements for NIST 800-171 and, when approved, CMMC.

There are a few main regulatory drivers which apply to CMMC:

- Federal Acquisition Regulation (FAR) guidelines (52.204 – 21) – These correspond to CMMC 2.0 Level 1 – Basic Cyber-hygiene. FAR (52.204 – 21) applies to ALL of the executive branch of the US Federal government. This FAR rule went into effect on 15 JUN 2016.
- The DoD has formalized a program and calls it CMMC 2.0 Level 1. Other executive branch agencies may follow this lead. Agencies from Homeland Security to the General Services Administration (GSA) have noted they are investigating using CMMC once it is finalized.
- Defense Federal Acquisition Regulation (DFAR) (252. 252.204-7012) Safeguarding Covered Defense Information and Cyber Incident Reporting. This DFAR procurement

rule that requires the contractor to implement the 110 NIST 800-171 controls went into effect in Nov 2017. The interim rule became permanent at the end of December 2022 meaning that enforcement and examination will be stepped up for every member of the DIB entering scores into SPRS (DoD's procurement system). This is another motivator for companies to partner with an MSP that can meet the NIST 800-171 cybersecurity requirements. This corresponds to CMMC 2.0 Level 2 Advanced.

- Executive Orders - There are several executive orders which also apply, including Executive Order 13556 -- Controlled Unclassified Information (4 NOV 2010) Likewise, the May 2021 EO 14028 – Improving the Nation's Cybersecurity is instructive. Software providers are significantly impacted if they sell software to agencies of the Federal government developed or with a major change after Sept. 12, 2022, then the seller must be able to provide an attestation at the top level of the organization of conformance to the Secure Software Development Framework. There was also an announcement by the Department of Justice that it would use the False Claims Act to assess whether a company that is invoicing the government has in fact met the cyber security rules. This puts a much greater onus on any organization seeking certification to get it right and the MSP is key on this point.

Market advantage

Accordingly, the opportunity 3Comply sees for MSPs is to develop the specific CMMC capability and then market themselves to all of these industry segments. Being a compliant early adopter is a significant advantage for retaining and obtaining new government related clients. The 3Comply principals have extensive MSP management background and worked in compliance for MSP contracts for close to 14 years each which informs this view.

MSP customers are becoming aware of the need to verify the provider's cybersecurity capabilities. External factors such as the war in Ukraine, threats from nation states, intellectual property theft, and a challenging financial marketplace are bringing these concerns to the forefront. Many customers rely upon MSPs to protect their infrastructure and intellectual property. This means that every company, regardless of whether it is in the government marketplace or not, is very concerned about security and how it is conducted by the firms outsourced to. Being able to demonstrate CMMC compliance is a way every company can clearly understand an MSP has made cyber security a top priority.

Basic – Level 1 CMMC and Enclave

We have found that formally attesting to every objective of Level 1 is not necessary for the whole company in many cases. This is especially true if there are a multitude of industry segments being serviced. The whole of the MSP itself can install the policies/procedures / processes necessary to operate in accordance with the CMMC framework at Level 1, without formally attesting. This would demonstrate basic cyber-hygiene to every current or future client.

At the same time, a smaller subset of clients that will require evidence of Level 1 (Federal Contract Information - FCI) compliance can be developed as an enclave within the greater company. This means an MSP can narrow the scope of assets including people and systems that would be subject to the formal attestation of compliance required to report in SPRS (the Supplier Performance Risk System used by the DoD). This would reduce the burden of meeting the stringent requirements to evidence CMMC Level 1 compliance based on the 59 objectives prescribed in the self-assessment guidance.

Board of Directors Confidence

Unlike other attestations such as SOC or ISO, the work to become CMMC Level 1 compliant, and report as such, is dependent on self-attestation. Due to liability considerations, most corporate boards prefer that the responsible senior manager have a report provided by an outside company known to be proficient in the area.

Of note: requirements for a US based enclave are not part of the CMMC framework. Any requirements for US based resources to be assigned to a client will be as a result of the client contract itself, and it is not an inherent part of the framework. This is a misconception many MSPs have but they are in fact, able to use non-US based resources unless the contract requires something else. Thus, an FCI (Level 1) enclave could be constructed to provide either US or non-US-resources, in our experience.

Level 2 CUI compliance

The requirements for Level 2 CMMC certification are much more stringent, as they focus on the protection of Controlled Unclassified Information (CUI) handled in a non-federal system. CUI is a broad category of information that may be marked or at times still unmarked by the government agency. Clients required to meet Level 2 could be serviced through an even smaller and tightly construed enclave dedicated to these customers. It is probably safe to say that many of the customers that would contract for this type of service would likely require US-based services including people and data centers.

Also of note is that some MSPs may elect to go directly to the CMMC Level 2 certification implementation. This makes sense if they already have several clients in the DIB that will most definitely have or want to have government contracts that will require CMMC Level 2 certification. Those clients will need their service provider to be able to evidence that controls can be inherited and be able to evidence controls are in place, fully implemented and monitored.

It is quite possible that a certified MSP will be able to charge a premium for providing services in a highly monitored and controlled enclave as well. This is something for consideration in your business case.

Training evidence that the CMMC program is making progress.

EVIDENCE
TO BE OPENED BY AUTHORIZED AGENTS ONLY
DO NOT USE THIS BAG WITH EVIDENCE THAT IS WET OR DAMP
Item #:
Time Sealed:
Cell #:

One approach we have found successful is to align training to the program steps as CMMC practices are being implemented over time. This approach enables an MSP to show its progress in installing segments of its CMMC program when that is requested or required for a current or future client. In today's environment, being able to show progress may well be enough to satisfy a future customer that you have sufficient plans in place to meet the CMMC requirement by the time the customer intends to bid on or wins a contract requiring it.

MSP Implementation Considerations

It is time to get started and lay out your plan. The certification program has already begun for members of the DIB who are voluntarily being assessed. My best guesses are that the first contracts with CMMC requirements will begin in May 2023. Build a timeline reflective of your current clients' needs and in keeping with the expected rollout plan. To take advantage of the DoD's plan, you will want to begin implementing in the first half of CY 2023. One key requirement is that operations must be able to demonstrate that the compliant method is how the organization that will be assessed (entirety or a defined enclave) operates.

Having a plan is particularly critical in order to ensure you have senior level commitment and designated budget by year end. Very few organizations have the bandwidth to stop and develop a plan, implement it, assess it, maintain a Plan of Actions and Milestones (POA&M), train and monitor for compliance from current resources and budget. Thus, budgeting is critical.

Calculating Return on Investment (ROI) is as straightforward as projecting revenue from new customers (potentially charged at a premium level for the enclave) against the costs of implementation over your standard amortization method. Your costs need to include new resources, monitoring for CMMC continuity and the ability to attest to your compliance level annually. This applies whether an MSP self-attests at Level 1 or being independently assessed for Level 2 and achieve certification. To improve the compliance standards, CMMC 2.0 requires an annual certification warranty by a senior level official via the SPRS score entered for CMMC compliance.

3COMPLY

Meet 3Comply:

- 3Comply is a Cyber-AB Registered Practitioner Organization (RPO). All staff as individuals are Cyber-AB Registered Providers (RPs) and Registered Provider Advanced (RPAs). This information is verifiable at the Cyber-AB Market place here: 3Comply Listing
- Managed Service Provider experience
- Having worked for large managed service providers for a collective set of 24+ years, the leaders of 3Comply also have extensive experience with the functions, methods of operation and compliance challenges on behalf of MSP clients. Each person has additional personal certifications and is well versed in the types of requirements regarding the security posture of a vendor (service provider) in terms of audit and assessment, external certifications (e.g., SOC 2 and ISO), MSP supply chain risk management, and expectations of clients.
- The working philosophy of 3Comply is “Comply Simply”. We have concluded that generally, people tend to overcomplicate procedures and processes that then make it difficult to be successful in an assessment or audit. Our stance is based on our years of experience in highly regulated industries including copious quantities of audits and assessments with government and non-government assessors and auditors.
- As key advisors, our approach with our clients is to assist in making the best decisions for their business and strategy based on risk and finances. As much as possible, we try to use our experience, and both ask the right questions and provide drafts of items for discussion rather than starting from a blank sheet.
- Contact us at comply@3comply.com or cmmc_help@3comply.com or 401.252.1800

3Comply’s Client Collaboration Model

- MSPs clearly have an opportunity to increase business or perhaps even change the culture of the company by embracing the CMMC model based on NIST 800-171. To get you there, you need to be able to count on the team you are working with to be knowledgeable, engaging, easy to work with and responsive.
- Our motto is to Comply Simply – a key compliance concept is that you have to say what you do and do what you say. If things are so complicated, or different from how you normally operate, you risk being unable to show an assessor that you really do what you say. We strive to make the CMMC readiness and implementation process as simple as possible while getting you where you need to be.

Reach out to us today! CMMC_help@3comply.com or 401.252.1800.